Mission-Function-Task Analysis for Cyber Defence

Melanie Bernier and Kathryn Perrett
Defence Research and Development Canada (DRDC)
101 Colonel By Drive, Ottawa, Ontario K1A 0K2
CANADA

Melanie.Bernier@drdc-rddc.gc.ca; Kathryn.Perrett@drdc-rddc.gc.ca

ABSTRACT

The decisions that must be made for cyber defence are often based on information that is both subjective and qualitative in nature. Objective, quantitative information can exist in the form of various measurements and metrics; however, it is not yet clear what information is needed to support the cyber defence decision-maker as the decision space for cyber defence has not been formalised. The NATO Communication and Information Agency (NCIA) Communications and Information System (CIS) Security Capability Breakdown presents a list of cyber defence capabilities and provides a useful starting point for such an analysis. As part of CIS security, cyber defence addresses the ability to safeguard the delivery and management of services in response to potential and actual malicious actions in cyberspace. In the present work, the breakdown of cyber defence capabilities is used to carry out a mission-function-task (MFT) analysis. This is accomplished by translating cyber defence capabilities into cyber defence missions and their functions, and then enumerating the tasks that would be needed to perform each function. The resulting tasks are then analysed for their information requirements in order to identify where measurements and metrics could support the decision-making needs. These results will contribute to unbiased decision-making by improving cyber defence situational awareness.

1.0 INTRODUCTION

The ability of cyber defenders to make rapid and accurate decisions depends on the quality and completeness of the available input information. Metrics that are objective, relevant, and robust can provide valuable support to decision making, although the types of cyber defence decisions and their related information requirements have not yet been formalised. The NATO Communication and Information Agency (NCIA) Communications and Information System (CIS) Security Capability Breakdown [1] presents a list of cyber defence capabilities and provides a useful starting point for conducting a functional analysis of cyber defence missions and the metrics that can ultimately be used to support them.

As part of CIS security, cyber defence addresses the ability to safeguard the delivery and management of services in response to potential and actual malicious actions in cyberspace [2]. A mission-function-task (MFT) analysis can be used to translate high-level cyber defence capabilities into major missions and the functions that are needed to achieve mission objectives. Functions are subsequently broken down into the individual tasks needed to perform them, and the resulting tasks are then analysed for their information requirements to help identify where measures and metrics may support decision-making needs. This type of analysis can be used to complement the gathering of stakeholder requirements by providing a more theoretical and comprehensive analysis of where metrics can serve to improve cyber defence situational awareness and the decision-making process.

The remainder of the paper is organised as follows. Section 2 summarises the MFT methodology and provides an overview of the steps used in the analysis. In order to define the list of capabilities upon which the analysis is based, a broad literature search was conducted to identify open source publications that enumerate cyber defence capabilities. The NCIA CIS security capability breakdown was used as the basis for the capability analysis, with additional capabilities added from the literature review, as described in Section 3. A preliminary MFT analysis was performed on the consolidated capability list as outlined in Section 4, which presents the derived tasks along with their major decisions, information requirements, and types of supporting metrics. Future work and a summary are provided in Sections 5 and 6, respectively.

2.0 MISSION-FUNCTION-TASK (MFT) METHODOLOGY

The MFT analysis methodology originates from the field of human factors engineering (HFE) and is part of the methodology used for assessing requirements in system development [3]. HFE analysis methods include mission analysis, function analysis, task analysis, and operational sequence analysis, although operational sequence analysis can be considered as part of task analysis. The analysis of missions is the first step in the identification and analysis of the functions that comprise them, and where the functions provide the basis for the subsequent task analysis.

- **Mission Analysis:** A mission includes the action required and its purpose [4]. A mission analysis provides information that defines the missions of the system, and the environment and circumstances in which these missions must be conducted. This analysis can include mission objectives as well as representative mission profiles or scenarios showing the major events and phases in mission execution [3].
- **Function Analysis:** A function is the broad, general, and enduring role for which an organisation is designed, equipped, and trained [4]. A function analysis identifies the functions (and sequence of functions) that must be performed for the system under analysis to achieve mission objectives. This analysis can include the creation of block diagrams, organisational charts, and flow charts, as well as the identification of critical paths and operation sequences [3][5].
- **Task Analysis:** A task is a discrete event or action that enables a mission or function to be accomplished [4]. Task analysis provides the basis for defining system requirements and can include the definition of information requirements, information availability, workload estimates, actions needed, and decision requirements [3][5].

In this paper we present the preliminary results from an MFT analysis for the missions and activities involved in cyber defence, which considers operations to defend the CIS. The mission analysis will define the cyber defence mission objectives and the environment in which the mission is conducted. The function analysis will then provide the high-level functions required to meet mission objectives, and will incorporate a functional decomposition of the mission from top-level cyber defence functions down to their lower level tasks. This analysis also provides an inventory of tasks that will be used as the basis for a subsequent analysis in which individual tasks—along with the decisions needed in accomplishing those tasks—will be defined. Information requirements will be determined based on those decisions, and the types of metrics that can be used to support or enhance decision making will be identified. The MFT analysis provides a theoretical approach to evaluating the information requirements for decision support in cyber defence, and this method is being used to validate and complement the collection of actual stakeholder metrics requirements via surveys and interviews [6].

3.0 LITERATURE REVIEW

The NCIA CIS security capability breakdown document has been in development since 2010 and is now in its fourth revision [1]. The NCIA breakdown was selected as the starting point for the MFT analysis as it provides a broad list of capabilities. To help ensure completeness, an extensive literature review was conducted to identify capability and functional breakdowns (or even lists of tasks) within the open literature. Most of the documents that were found contained only contextual background information, while a few provided specific capabilities and tasks that could be incorporated in the MFT analysis. These additional capabilities were evaluated against—and, where appropriate, incorporated in—the consolidated lists as part of the analysis process described in Section 4.

3.1 NCIA CIS security capability breakdown

The NCIA CIS security capability breakdown was originally produced as a cyber defence capability framework, but has since evolved to include all of the areas of communications and information system security. The objective of the NATO CIS security capability breakdown is to create a foundation for CIS security and cyber defence capability development within NATO and member nations by defining key terms, and by presenting and organising capabilities for use in a variety of applications.

Revision 4 of the NCIA document is the most current version, with one of the main differences from previous versions being that it no longer refers to cyber defence as a separate entity within the capability breakdown [1]. Cyber defence capabilities have now been integrated into the wider CIS security framework, mostly under the "Operate CIS Security" capability. In Revision 3 of the NCIA document [2], cyber defence capabilities are defined as being part of CIS security but are still presented as a separate entity. As the MFT analysis in this paper is primarily concerned with cyber defence capabilities, the remainder of this document refers just to the portion of the CIS security capability breakdown presented in Annex B of Revision 3 (in [2]) and as shown below in Figure 1.

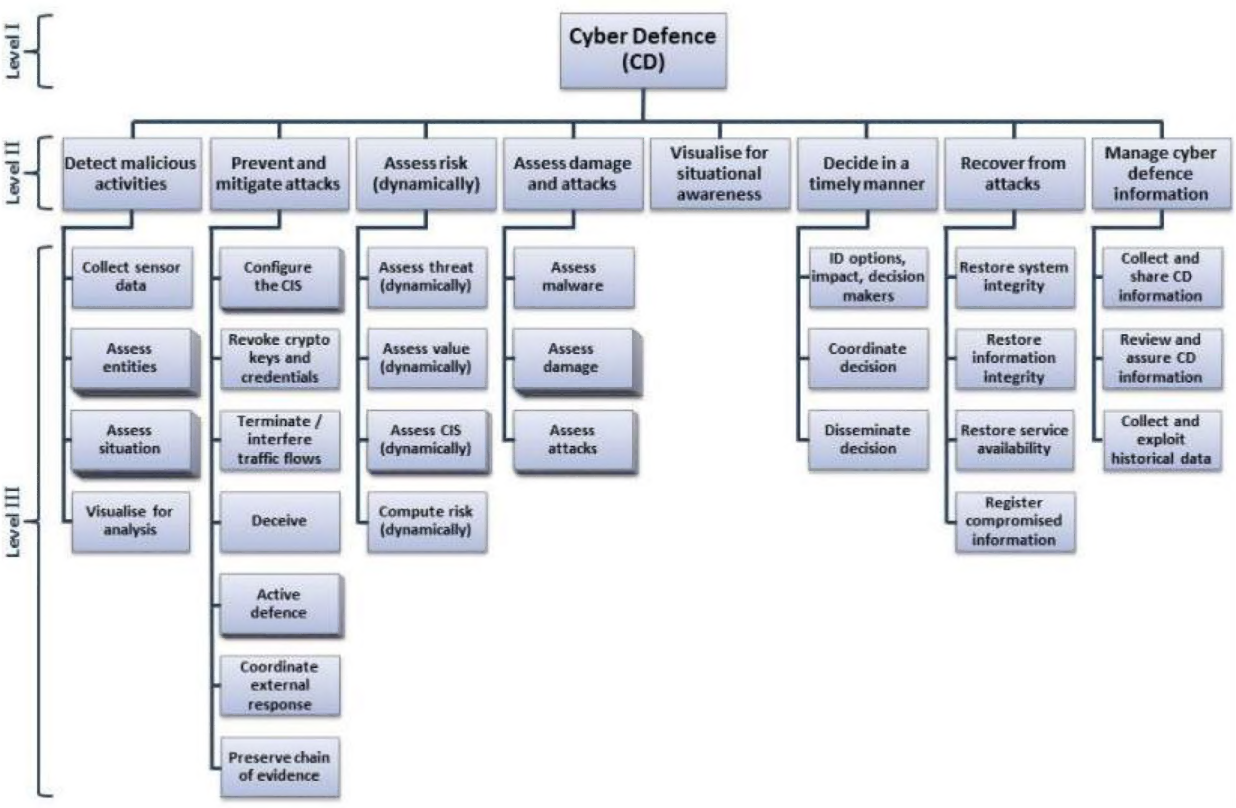
Level I
Level II
Level III
Cyber Defence (CD)
Detect malicious activities
Prevent and mitigate attacks
Assess risk (dynamically)
Assess damage and attacks
Visualise for situational awareness
Decide in a timely manner
Recover from attacks
Manage cyber defence information
Collect sensor data
Assess entities
Assess situation
Visualise for analysis
Configure the CIS
Revoke crypto keys and credentials
Terminate / interfere traffic flows
Deceive
Active defence
Coordinate external response
Preserve chain of evidence
Assess threat (dynamically)
Assess value (dynamically)
Assess CIS (dynamically)
Compute risk (dynamically)
Assess malware
Assess damage
Assess attacks
ID options, impact, decision makers
Coordinate decision
Disseminate decision
Restore system integrity
Restore information integrity
Restore service availability
Register compromised information
Collect and share CD information
Review and assure CD information
Collect and exploit historical data

Figure 1: NCIA CIS cyber defence capability breakdown [2].

3.2 Additional capabilities from the literature

The additional documents that were reviewed for the analysis pertained to the cyber security and/or defence of countries including Australia, Canada, Czech Republic, Estonia, Finland, Netherlands, Norway, Spain, Sweden and the United States. Documents from countries with existing operational capabilities for cyber security and cyber defence[1] (specifically those from the US) tend to be more in depth, and are more likely to contain information regarding tactics, techniques, and procedures (TTPs), or to provide well-defined lists of capabilities or tasks. Other countries that are currently building national capabilities for cyber security and cyber defence (e.g., Canada and Australia) are typically progressing past the conceptual phase into implementation, and are more likely to be developing the functional aspects of their cyber capabilities. Documents from countries that are in the process of defining (or have not yet begun to define) national cyber capabilities are typically not at a sufficiently advanced stage to provide more than contextual information (e.g., white papers and national strategies for cyber security). Also considered were documents from intergovernmental alliances such as NATO, the European Defence Agency (EDA), the European Commission, the Council on Cybersecurity and the Consortium for Cybersecurity Action (CCA).

Several cyber-related taxonomies were discovered during the course of the literature search. Some of the more common taxonomies for computer network defence software and hardware tools are reported in [8] and include host-based or network-based systems, honeypots, as well as intrusion detection systems (IDSs) that are signature-based and anomaly-based. Other related taxonomies or classifications that were examined include a cyber defence of computer networks ontology [9], a

[1] The categories of national capabilities are based on the four groups described in [7].

cyber challenges taxonomy [10], and a paper considering United States cyber competitions [11]. While these provided useful perspective and additional details, none were sufficiently complete to compare directly to the NCIA CIS security capability list. The two most relevant cyber security taxonomies found in the literature present listings of functions that are categorised into jobs and further delineated into tasks. These documents are the CyberSkills Task Force Report from the Homeland Security Advisory Council (HSAC) [12] and the National Cybersecurity Workforce Framework by the National Initiative for Cybersecurity Education (NICE) [13]. The HSAC CyberSkills Task Force Report outlines specific jobs along with a description of the tasks and their accompanying consequences for failure to perform. The NICE National CyberSecurity Workforce Framework contains functional groupings of jobs, complete with very detailed sets of task, knowledge, and attitude statements for each job.

The most relevant cyber defence publications found in the national and allied literature were the United States Department of Defence's Universal Joint Task List (UJTL) [14], Canada's Department of National Defence and the Canadian Armed Forces (DND/CAF) Chief of Force Development's (CFD) capability framework [15][16], as well as DND/CAF Directorate of Cyber Force Development's (D Cyber FD) draft functional concept for Defensive Cyber Operations [17] and draft CAF Cyber Operations Primer [18]. The UJTL document provides a menu of tasks in a common language, and serves as the foundation for joint operations planning across the range of military and interagency operations. CFD's capability framework presents a hierarchical structure in which each level (Domain, Capability, Function, Activity, Subactivity) is comprised of a set of elements. The D Cyber FD documents currently exist in draft form and do not define the approved way ahead for Canada; however, they do include a list of capabilities and definitions that are currently being considered for cyber defence. These capabilities and definitions provide a useful basis for comparison with those from the NCIA document and the US UJTL, and will be incorporated in the cyber defence capability assessment in order to ensure alignment with Canada's proposed way ahead in cyber defence. The creation of a consolidated list of cyber defence capabilities will be described in the next section.

4.0 RESULTS

An MFT analysis was conducted on the list of capabilities gathered from the literature review (described in Section 3) in order to obtain a theoretical perspective on the decision-making requirements for cyber defence. The results from the analysis presented in this section will serve to supplement requirements that were collected directly from cyber defence stakeholders via surveys and interviews [6], and will provide a more comprehensive assessment of the decision maker's needs. Examining the NCIA CIS security capability breakdown in Figure 1 as a starting point for the analysis: the Level I capabilities are equivalent to the mission level, and the subordinate Level II capabilities as functions that enable the completion of the mission. The Level III capabilities and below are being treated as tasks and sub-tasks where applicable. This paper presents the preliminary results for the first three levels of capabilities, and describes the results for several elements at each level of analysis (mission, function, and task) for illustrative purposes.

4.1 Mission analysis

The objective of the mission analysis is to define the missions for cyber defence (the Level I capability) as well as the environment and circumstances in which these missions must be conducted. The following definitions were considered in forming the mission statement.

- **Cyber defence** (NCIA): "The ability to safeguard the delivery and management of services in an operational CIS in response to potential and imminent as well as actual malicious actions that originate in cyberspace" [2].

- **Cyber defence** (DND/CAF D Cyber FD): "Measures designed to nullify or reduce the effectiveness of hostile action in the cyber environment" [17].
- **Defensive cyber operations** (DND/CAF D Cyber FD): "Cyber operations to defend friendly cyber capabilities, including data, necessary to maintain a commander's situational awareness and the ability to employ forces" [18].

The mission objective for cyber defence is therefore *to gain and maintain superiority within the cyber environment in order to assure friendly-force freedom of action* [17]. The mission includes the activities conducted before, during, and after an attack to prevent or stop the adversary actions, and to restore the reliability and availability of the CIS. According to DND/CAF, the cyber environment is defined as "the interdependent networks of IT structures, including the Internet, telecommunications networks, computer systems and embedded controllers, as well as the software and data that reside within them" [18]. The effects of actions taken within the cyber environment also impact the other operating environments (air, land, sea, and space), as networked systems or nodes also physically reside on board vehicles, ships, aircraft, and satellites [18].

4.2 Function analysis

The objective of a function analysis is to identify the functions (and sequence of functions) that must be performed by the system in order to achieve mission objectives. The Level II capabilities listed under cyber defence (CD) in the NCIA document [2] provided a starting point for this analysis. Capabilities listed as part of the draft Functional Concept paper for Defensive Cyber Operation (DCO) currently in development within the D Cyber FD [17] were compared against the NCIA list. The functional capabilities defined in these two documents are presented in the first two columns of Table 1, each row representing the capabilities that were identified as being related based on their definitions and associated activities. Note that a blank cell within the table indicates that the particular capability is represented in only one of the two documents. Linked capabilities were then combined wherever possible and were renamed based on the context of current DND/CAF directions [17][18]. The consolidated list of functional capabilities was then reordered to better reflect the sequence in which they are typically executed; i.e., within the Observe, Orient, Decide, and Act (OODA) phases of the military decision-making process. The final column of Table 1 provides the consolidated list of cyber defence capabilities in sequence of execution.

Table 1: Comparison and consolidation of NCIA and D Cyber FD functional capabilities.

NCIA CD Level II Capabilities	D Cyber FD draft DCO Capabilities	Consolidated CD Capabilities
□	Protect systems and networks	Protect systems and networks
Detect malicious activities	Monitor systems and networks Detect adversary action	Monitor and detect adversary action

Assess risk	□	Assess risk
Assess damage and attacks	Analyse incident information and data	Analyse attacks and assess impact
Visualise for situational awareness Decide in a timely manner Manage cyber defence information	Command and control Cyber Forces Communicate command direction	Provide command and control (C2)
Prevent and mitigate attacks Recover from attacks	Respond to adversary action	Respond to adversary action
□	Anticipate future requirements	Anticipate future requirements

The consolidated capability list (Column 3 of Table 1) then becomes the list of functions that will be used in the next stage of the MFT analysis. These functions are described below.

1. **Protect systems and networks**: The ability to protect networks and systems from incidents and attacks is the essence of cyber security, which itself is aimed at safeguarding system availability, integrity, authentication, confidentiality, and non-repudiation [17]. As a security function, protection is not included in the NCIA cyber defence capability list, although it is included in the broader NCIA CIS security capability breakdown. Since it is part of cyber security and not cyber defence, protection will be excluded from the next step of this analysis, which involves the decomposition of the functions into an inventory of tasks.
2. **Monitor and detect adversary action**: The ability to sense for and detect adversary action on systems and networks will allow for the planning of response courses of actions [17]. This can be achieved by collecting sensor information, recognising actions through the assessment of entities, understanding activities in both local and global contexts by assessing the situation, and providing visualisation for human analysts to enhance detection [2].
3. **Assess risk**: The ability to assess threats, values, and the CIS, and to compute the risk to the CIS based on the assessments and relevant cyber defence information [2].
4. **Analyse attacks and assess impact**: The ability to assess the damage incurred from attacks and to improve the understanding of threats by assessing malware and attacks [2].
5. **Command and control**: The ability to develop an understanding of the situation, develop potential solutions, select a course of action, issue the commander’s intent and orders, monitor the execution of operations, and evaluate the results [19].
6. **Respond to adversary action**: The ability to respond to adversary action and to remove their influence on systems and networks. Response includes the ability to prevent, mitigate and recover from adversary action as well as to preserve the chain of evidence for use in prosecution [2][17].
7. **Anticipate future requirements**: The ability to anticipate how requirements affect all aspects of capability development. Capabilities must be developed to house, maintain, train, deploy, and sustain future assets [17]. This function is not included in the task analysis as it is part of future requirements and as such the tasks are not yet defined.

As described above, five of the functions (numbers 2 through 6) will be considered in the subsequent functional decomposition in order to identify related tasks. The NCIA capability list was redistributed to fit within these new categories of functions, where some of the NCIA Level II capabilities become Level III capabilities under the new set of functions (see *command and control*, and *respond to adversary action*). The combined list of capabilities was then supplemented with other tasks from the literature review discussed in Section 3.

In order to consider the tasks included in the HSAC and NICE documents, those lists needed to be modified to include the same level of granularity as the NCIA reference document. This step required breaking down the HSAC listing into more specific tasks, while rolling up the NICE listings into higher level tasks. In the end, while only seven task statements from these two documents were added to the final task lists, the comparison did serve to confirm the comprehensiveness of the NCIA list.

The tasks and activities from the US UJTLs and the Canadian documents were also compared to the original task list derived from the NCIA document, and a few additional tasks were again added to the final task list. Again, many of the tasks described in these documents already existed in some form within the NCIA capability list. In the Canadian capability framework the relevant capabilities considered were computer network defence and command and control, while for the UJTLs the following tasks were specifically considered:

- SN 5.5.11: Manage Cyberspace Operations;
- SN 5.5.3: Provide Defensive Cyberspace Operations (DCO);
- SN 5.5.5: Defend the Department of Defense Information Networks (DODIN);
- ST 5.5.7.3: Direct Computer Network Defense was assessed;
- OP 5.1.3: Determine Commander's Critical Information Requirements (CCIRs);
- OP 5.4.7: Integrate Computer Investigations and Operations in Computer Network Defense;
- OP 5.6.5.3: Conduct Defensive Cyberspace Operations (DCO); and
- TA 5.6.5.3: Execute Defensive Cyberspace Operations (DCO).

Table 2 presents the tasks that were added to those described in Annex B of [2] in order to fill the observed gaps, thereby producing the final task list to be assessed in Section 4.3. Figure 2 shows the new representation of consolidated capabilities down to Level III.

Table 2: Tasks added to those in Annex B of [2]

Function	Task Additions	Reference
Monitor and detect adversary action	Develop detection techniques and tools	HSAC [12], p.8

• Monitor systems and networks		
Monitor and detect adversary action • Assess Entities	Identify indicators	HSAC [12], p.7
Respond to adversary action • Prevent and mitigate adversary action □ Active defence	Develop and deploy eradication tools	HSAC [12], p.7
Respond to adversary action • Prevent and mitigate adversary action □ Preserve chain of evidence	Balance prosecution versus intelligence gathering	NICE [13], p.9
Respond to adversary action • Prevent and mitigate adversary action □ Preserve chain of evidence	Identify key information	HSAC [12], p.8
Analyse attacks and assess impact • Assess malware	Reverse engineer	HSAC [12], p.7
Analyse attacks and assess impact • Assess attack	Group threat actors	HSAC [12], p.8
Analyse attacks and assess impact • Assess attack	Conduct forensic analysis	D Cyber FD [17]
Command and Control	Plan course of action	CA C2 CBP [16]
Command and Control	Organise and Coordinate Decision	CA C2 CBP [16]
Command and Control • Organise and Coordinate Decision	Determine Commanders Critical Information Requirements (CCIRs)	UJTL [14]
Command and Control • Organise and Coordinate Decision □ Determine CCIRs	Determine Operational Cyber Priority Intelligence Requirements (PIRs)	D Cyber FD [17]
Command and Control • Organise and Coordinate Decision □ Determine CCIRs	Determine Operational Cyber Information Requirements (IRs)	D Cyber FD [17]
Command and Control • Organise and Coordinate Decision	Determine information relevance	CA C2 CBP [16]
Command and Control • Organise and Coordinate Decision	Manage the battlespace	CA C2 CBP [16]
Command and Control	Direct course of action	CA C2 CBP [16]
Command and Control • Direct course of action	Issue orders	CA C2 CBP [16]
Command and Control	Control forces	CA C2 CBP [16]

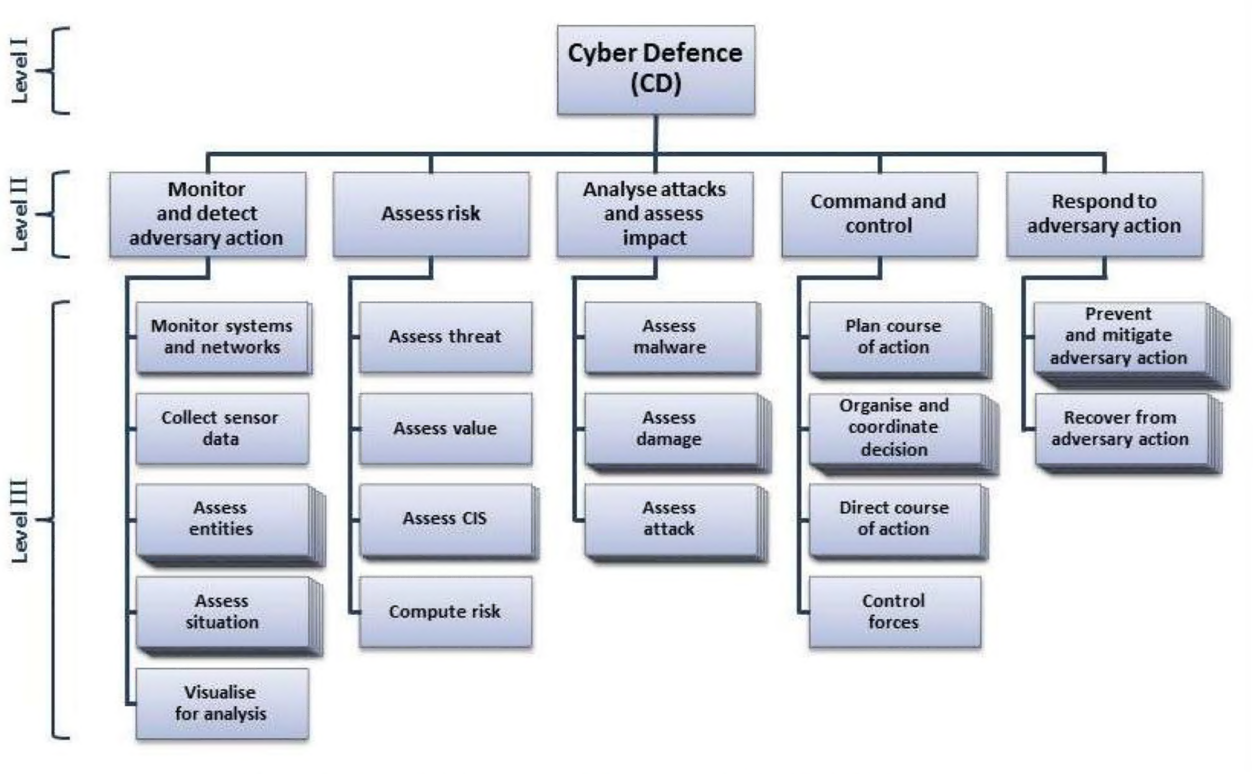

Figure 2: Consolidated cyber defence capability breakdown.

4.3 Task analysis

The primary objective of the task analysis is to develop a database of task-related information to support the requirements for decision making in cyber defence. This analysis will complement the collection and analysis of metrics requirements that is being conducted as part of the Security and Defence Metrics component of the Cyber Decision Making and Response (CDMR) project under the Cyber Operations S&T Program within Defence Research and Development Canada (DRDC) [6]. Using the list of tasks that was derived through the function analysis, the task analysis consists of defining a set of data elements for each unique task that includes the following components:

- Task description;
- Decisions to be made in performing the task;
- Information required in making the decision; and
- Types of metrics that can support information requirements and decisions.

Although the MFT analysis effort will include the complete list of tasks and subtasks determined through the function analysis in Section 4.2, only the first level of tasks will be discuss in this section (i.e., Level III of the new consolidated capability list presented in Figure 2). Functions in the cyber defence mission are enumerated from CD-1 to CD-5, and their tasks are enumerated as CD-1.1, CD-1.2, etc. The boxes following each task present their major decisions, information requirements, and supporting metrics types.

CD-1 Monitor and detect adversary action

CD-1.1 Monitor systems and networks: Sense network traffic for ongoing and previously executed adversary action both at the network perimeter and within the network itself [17].

Decision Required	Information Required	Supporting Metrics
What tools and techniques are required to monitor systems and networks?	Existing and available tools and techniques Network architectures and systems to be monitored Knowledge base of previously identified adversary action	N/A
Do new tools and techniques need to be acquired or developed?	Existing and available toolsets Capability gaps and assessments	N/A

CD-1.2 Collect sensor data: Collect data on all ongoing activities as well as the state of all relevant CIS components in a comprehensive repository through the use of sensors and the alignment of syntax and common reference points for that data [2].

Decision Required	Information Required	Supporting Metrics
What types of sensors are needed to support monitoring (CD-1.1); how should they be placed and configured?	Network architectures and systems to be monitored Governance of networks and systems Data collection policies and directives	N/A
What data (network traffic, system logs) need to be recorded and retained?	Data collection policies and directives Storage capacity and retention policies Lessons learned from past incidents	N/A

CD-1.3 Assess entities: Identify entities[2] by fusing sensor data from multiple different sensors through the semantic alignment of the sensor data, the correlation between sensor data to recognise entities representing actions, estimation of the entity attributes, and characterisation of the entity with respect to type of action and nature (benign/fault/malicious) [2].

Decision Required	Information Required	Supporting Metrics
Can an entity (i.e., action) be identified from the sensor data?	Outputs from multiple sensors Completeness and validity of sensor data	Traffic characterisation and anomaly detection Sensor data correlation Sensor performance and coverage

[2] Examples of entities can include port scans, email reception, download of a web page, etc.

What is the type and nature of the entity?	List of characteristics of various known actions Knowledge base of previously identified entities CIS component and information usage	Usage baselines / anomaly detection Threat characterisation

CD-1.4 **Assess situation:** Identify activities by assessing the relationships between entities, the technical source of the activity, the comprehension of the intent behind the activity, and the understanding of the activity's meaning in a global context [2].

Decision Required	Information Required	Supporting Metrics
Can some of entities be linked in any way to form an activity?	Entities that have been identified and their characteristics (type and nature) Timing and sequence of entities Knowledge base of previously identified entities and their correlations	Trend analysis and prediction
Can the technical source[3] of the activity be identified?	Network traffic data (type, origin, destination) Adversary TTPs	Threat characterisation

CD-1.5 **Visualise for analysis:** Present and visualise activities, actions, entities, and sensor data in order to support human analysts in detecting malicious activity [2].

Decision Required	Information Required	Supporting Metrics
What data is required by the analysts?	Analyst roles and responsibilities Analysis techniques to be used	N/A
What tools should be used to view and process the information collected and identified?	Data to be included, and methods to be used in the processing and analysis Analysis techniques requirements (e.g., drill-down, customisation)	N/A

CD-2 Assess risk

CD-2.1 **Assess threat:** Analyse malicious threat sources and evaluate their intent and capability [2].

Decision Required	Information Required	Supporting Metrics
What people, processes, and technologies (PPTs) are needed to analyse the threat?	Knowledge level and expertise of personnel. Purpose and performance evaluations for processes and technologies	PPT performance
What is the nature of the threat?	Threat characteristics: type, location, TTPs, targets	Source-based statistics (e.g., threat capability,

[3] Technical source refers to control server or origin of the activity.

	Trends and previously executed actions	targeting) Trend analysis and prediction

CD-2.2 **Assess value:** Analyse and evaluate the value to the mission of information processed, stored, or transmitted by the CIS, the services provided by the CIS, and the CIS itself [2].

Decision Required	Information Required	Supporting Metrics
What is the value of the information to the mission?	Mission objectives and commanders intent Information flow diagrams and user requirements	Asset valuation and impact
What is the value of the services to the mission?	Mission objectives and commanders intent	Asset valuation and impact

CD-2.3 **Assess CIS:** Identify vulnerabilities and assess dependencies in CIS designs and components [2].

Decision Required	Information Required	Supporting Metrics
What are the vulnerabilities of the CIS components?	Known vulnerabilities (databases) Network and system configurations Safeguards and controls	Vulnerability Resilience Compliance
Are there any dependencies between the CIS components?	Network maps and system configurations Information flow and traffic patterns	N/A

CD-2.4 **Compute risk:** Calculate the risk based on the analysed threats, values, and the vulnerabilities and dependencies in the CIS and its components [2].

Decision Required	Information Required	Supporting Metrics
What CIS-based risks will affect the mission?	Mission objectives and commanders intent CIS component performance, vulnerabilities, and dependencies CIS and information value to the mission Threat and impact assessments	Network and system health Cyber security risk (based on vulnerability, threat, and impact)

CD-3 Analyse attacks and assess impact

CD-3.1 **Assess malware:** Analyse malware in order to understand its function and the damage it may cause or has caused, as well as to understand the sophistication of malware for the purpose of improving threat assessment [2].

Decision Required	Information Required	Supporting Metrics
What is the nature of this malware?	Lists of known malware and their behaviours Reverse engineering and forensics analysis results Observed effects and incident reports	Vulnerability and software engineering Impact and damage assessment

CD-3.2 Assess damage: Identify affected systems, verify the integrity and availability of systems and information, and identify any compromised information caused by an attack [2].

Decision Required	Information Required	Supporting Metrics
What systems, services and/or information have been affected by the attack?	System and service logs Performance and availability of CIS components Incident reports	Performance Damage assessment
Was the information compromised in any way?	Document metadata and access logs File integrity verifications	N/A

CD-3.3 Assess attack: Analyse attacks, including the coordination of external monitoring, in order to gain insight into the attacker's intent and capability and attribution [2].

Decision Required	Information Required	Supporting Metrics
Should we allow the attack to progress in order to gain more information on the attack?	Information already captured on the attack internally or externally Network maps and system configurations Threat assessments, including adversary TTPs	Exposure and resiliency Damage assessment (predictive)
Is this attack also occurring on external partners systems and networks?	Type of attack Technical source of the attack	Damage assessment

CD-4 Command and control

CD-4.1 Plan course of action (CoA): Assess the factors that are critical to supporting course of action selection in order to exploit opportunities or respond to rapidly developing situations [19].

Decision Required	Information Required	Supporting Metrics
What are the possible CoAs?	Mission objectives CIS infrastructure and components Results of attack analysis and threat assessments, including adversary TTPs	N/A

What is the appropriate course of action?	Mission objectives and context The “what, why, where, when, and by whom” of possible CoAs Results from risk assessments	CoA alignment Capability coverage and performance Cyber security risk (based on vulnerability, threat, and impact).

CD-4.2 Organise and coordinate decision: Determine the roles and responsibilities and the resources required to execute course of action. Align actions and effects with the commander’s intent to achieve mission objectives. Coordinate decision between elements of military forces and other organisations or agencies to ensure mutual understanding and unity of purpose and effort [19].

Decision Required	Information Required	Supporting Metrics
What is needed to implement the course of action?	Mission objectives and operational priorities, including CCIRs, PIRs, and IRs CIS infrastructure and components, safeguards Available resources, processes, and tools Roles and responsibilities of personnel	PPT performance Resource management
How is information being shared to coordinate the decision?	Stakeholder entities and organisations Roles and responsibilities of personnel Information related to CoA	Information sharing performance (relevance, accuracy, usability, timeliness)

CD-4.3 Direct course of action: Issue orders and instructions to those with a role in accomplishing the mission [19].

Decision Required	Information Required	Supporting Metrics
How well has the directed course of action been communicated and understood?	Orders and instructions for accomplishing the CoA Roles and responsibilities of personnel Acknowledgement/confirmation of orders received	Shared understanding (e.g., correctness, completeness, timeliness)

CD-4.4 Control forces: Monitor, assess situation and progress, and establish and apply the necessary means to ensure that plans, orders and policies are complied with in such a manner that the desired effects will be attained [19].

Decision Required	Information Required	Supporting Metrics
How is the course of action progressing?	Situational awareness and common operating picture Progress made towards established outcomes Resource allocation	CoA alignment Correctness, completeness, and timeliness of actions Resource management

What is needed to ensure that the desired effects will be attained?	Mission objectives and Commander’s intent Time, effort, and resources needed to correct CoA	Performance and compliance Resource management Synchronisation (adaptability and flexibility)

CD-5 Respond to adversary action

CD-5.1 Prevent and mitigate adversary action: Prevent and mitigate the effect of adversary actions through CIS component configurations and updates, cryptographic key and credential revocation, manipulation of traffic flows, deception, active defence, coordination of external responses, and preservation of the chain of evidence for the purpose of prosecution [2].

Decision Required	Information Required	Supporting Metrics
How should CIS components be configured to prevent adversary actions?	Network and system components and architectures. Vulnerabilities and patching requirements. Security control profiles (NIST 800-53, ITSG-33)	Vulnerability, defensive posture, and exposure Configuration and patch management Compliance and performance
What steps are required to mitigate the adversary action?	CoA selected Threat assessments, including adversary TTPs Dependencies and effects on systems and missions	Game theoretic measures Asset valuation and impact assessments

CD-5.2 Recover from adversary action: Restore system and information integrity, CIS service availability, and register any compromised information [2].

Decision Required	Information Required	Supporting Metrics
What, if any, of the information/data have been compromised?	System logs, sensor data, and incident reports Information assets and system dependencies Results of integrity checks	Security incident management Information integrity
Can the restored systems and information be trusted?	Systems and information assets affected Integrity and availability of backup systems and information System and information assets, and value to mission	System integrity Information security risk

5.0 DISCUSSION AND FUTURE WORK

This preliminary analysis of cyber defence capabilities and their functional breakdown into tasks provided a structured means of investigating information and metrics requirements for the types of decisions needed. Only a partial MFT analysis was completed for the preliminary analysis in this paper, with the next steps involving the development of scenarios/vignettes as part of the mission analysis stage. These scenarios will be used in table-top exercises to validate the functions and perform a more complete cyber defence task analysis. These table-top exercises will include participation from military operators as well as other cyber defence stakeholders and experts. The results will provide a more complete list of tasks and information requirements in alignment with DND/CAF's current directions in cyber operations [18].

The resulting task list and information requirements will be used as part of an ongoing DRDC effort to define meaningful and robust metrics for use in cyber defence. The objective of this research activity is to provide rigorous measures of cyber defensive posture, active threats, dynamic asset valuation, and damage assessments as input to risk analysis and decision making. In addition to gathering and assessing specific stakeholder requirements and their current decision-making gaps, a more formalised and complete view of potential tasks in cyber defence can provide valuable insight into requirements for decision making. The information requirements associated with the tasks and sub-tasks derived from the finalised MFT analysis will be used to develop a comprehensive cyber defence metrics framework that will supplement metrics requirements gathered from specific stakeholders [6].

6.0 SUMMARY

Cyber defence metrics can provide valuable input to situational awareness and decision making, although defining a comprehensive set of appropriate and meaningful metrics demands a better understanding of the tasks and information requirements of potential decision-makers. This paper presents the preliminary results of a mission-function-task analysis used to translate cyber defence capabilities into the tasks needed to achieve mission objectives. The NCIA CIS security capability breakdown was used as the starting point for defining cyber defence capabilities. These capabilities and others identified from the literature were combined and considered within the context of current DND/CAF directions in cyber defence operations in order to define the relevant missions and their component functions. The resulting functions and their associated tasks were consolidated and aligned with current DND/CAF processes and terminology, and were then reordered to reflect the sequence in which they are typically executed (i.e., in accordance with the OODA phases of the military decision-making process). The resulting tasks were analysed for their supporting decisions and information requirements in order to identify where metrics can help to improve decision making in cyber defence. Follow-on work using mission scenarios/vignettes within table-top exercises will help to formalise the set of decisions required within cyber defence, and these decisions can be used to build a more comprehensive framework of supporting metrics.

[1] Hallingstad, G., and Dandurand, L., "Communication and Information System Security Capability Breakdown", Rev. 4, NATO Communications and Information Agency (NCIA), The Hague, August 2013.

[2] Hallingstad, G., and Dandurand, L., "Communication and Information System Security Capability Breakdown", Rev. 3, NATO Consultation, Command and Control Agency, The Hague, November 2011.

[3] Engel, R., "User Manual: Guidelines for Human Factors Engineering Requirements for Canadian Forces Command and Control Information Systems", DCIEM No. 98-CR-20, DRDC Toronto, Department of National Defence, Government of Canada, April 1998.

[4] US Joint Chief of Staff, "Doctrine for the Armed Forces of the United States", Joint Publication 1, Department of Defence, United States, 25 March 2013.

[5] Baker, K., and Youngson, G., "Advanced Integrated Multi-sensor Surveillance (AIMS): Mission, Function, Task Analysis", DRDC Atlantic CR 2007-21, Department of National Defence, Government of Canada, June 2007.

[6] Perrett, K., Bernier, M., and Treurniet, J., "Metrics Requirements for Decision Support in Cyber Defence", Defence Research and Development Canada, NATO SAS-106 Symposium, May 2014.

[7] The Cybersecurity Think Tank, "Cyber Cells: A Tool for National Cybersecurity and Cyberdefence", ARI 26/2013, Real Instituto Elcano, 17 September 2013.

[8] Garcia, A., and Aranda, N., "D1.3 Report on Technology Taxonomy and Mapping", ATOS, Spain, 5 June 2012.

[9] Kaderka, J., "Ontology in Cyberdefence and Computer Networks", Cybernetic Letters, Special Issue, December 2010.

[10] Winterfeld, S., "Understanding Today's Cyber Challenges", White Paper, TASC Inc., Virginia, United States, May 2011.

[11] Kay, D.J., Pudas, T.J., and Young, B., "Preparing The Pipeline: The U.S. Cyber Workforce for the Future", Defense Horizons, INNS, National Defense University, August 2012.

[12] Homeland Security Advisory Council, "CyberSkills Task Force Report", Department of Homeland Security, United States of America, Fall 2012.

[13] National Initiative for Cybersecurity Education (NICE), "The National Cybersecurity Workforce Framework", http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf (accessed 11 May, 2014).

[14] Joint Electronic Library, "Approved Universal Joint Task List (UJTL) database", Department of Defence, United States, 13 March 2014.

[15] Rempel, M., "An Overview of the Canadian Forces' Second Generation Capability-Based Planning Analytical Process", DRDC CORA TM 2010-198, Department of National Defence, Government of Canada, September 2010.

[16] Rempel, M., "Visualizing Capability Requirements", DRDC CORA TR 2013-068, Department of National Defence, Government of Canada, May 2013.

[17] Directorate of Cyber Force Development, "Defensive Cyber Operations Functional Concept (Draft Version 1.0)", Chief of Force Development, Department of National Defence, Government of Canada, July 2013.

[18] Directorate of Cyber Force Development, "CAF Cyber Operations Primer (Draft Version 1.0)", Chief of Force Development, Department of National Defence, Government of Canada, December 2013.

[19] Chief of Force Development, "Command and Control Operating Concept (Draft)", Department of National Defence, Government of Canada, December 2011.